STRATEGY RESEARCH PROJECT

BOUNDED RATIONALITY AND COMPLEX PROCESS COUPLING: CHALLENGES FOR INTELLIGENCE SUPPORT TO INFORMATION WARFARE

BY

COLONEL KEVIN R. CUNNINGHAM
United States Army

USAWC CLASS OF 2000

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

USAWC STRATEGY RESEARCH PROJECT

Bounded Rationality and Complex Process Coupling: Challenges for Intelligence Support to Information Warfare

by

Colonel Kevin R. Cunningham
U.S. Army

Dr. David Jablonsky
Project Advisor

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Kevin R. Cunningham

TITLE: Information and Understanding: Structural Challenges for Intelligence Support to Information Operations

FORMAT: Strategy Research Project

DATE: 10 April 2000 PAGES: 48 CLASSIFICATION: Unclassified

Information warfare is predicated on a belief that new information processing technology, that has been embedded in intelligence surveillance and reconnaissance systems, command and control systems, and precision munitions, has vastly increased U.S. military capabilities. Systems employing information technology are believed to allow the attainment of information superiority and consequently enable dominant maneuver across the "battlespace." Information warfare places heavy responsibility on the intelligence which is collected and processed through these systems. However, information warfare doctrine reveals an idiosyncratic interpretation of intelligence which favors indicators from reconnaissance and surveillance systems and discounts the value of intelligence analysis. The bias favoring surveillance and reconnaissance products reflects unrealistic expectation regarding the perfectibility of this type of intelligence. Furthermore, using the concepts of bounded rationality and complex process coupling from organization theory, the paper argues that decision makers require a balanced input of surveillance and reconnaissance products and intelligence analysis if they are to develop a real understanding of complex strategic interactions. Intelligence analysis will also help reduce the possibility that systems accidents will occur when surveillance and reconnaissance sensors are tightly coupled with weapons systems. The paper offers a balanced approach to the relationship between intelligence analysis and information warfare to properly account for the effects of bounded rationality and complex process coupling.

TABLE OF CONTENTS

PREFACE

I am extremely grateful for the intellectual and editorial support I received from Dr. David Jablonsky and Major Linda L. Cunningham, USAR.

BOUNDED RATIONALITY AND COMPLEX PROCESS COUPLING: CHALLENGES FOR INTELLIGENCE SUPPORT TO INFORMATION WARFARE

They constantly try to escape
From the darkness outside and within
By dreaming of systems so perfect that no one will need be good.
T. S. Eliot, "The Rock"

The technologically astonishing Gulf War against Iraq led many scholars to speculate that advances in information related technology were producing major changes in the nature of war. These ideas were not new since the various relationships between science, technology, politics, war, strategy and military organizations have been thoroughly studied, particularly since World War II.[1] What seemed different about the situation after the Desert Storm operation, however, was the broadly shared impression that information technology had imposed potentially "revolutionary" changes that were many orders of magnitude more pervasive and significant than had been previously anticipated.[2] Furthermore, a great strategic opportunity was available to the United States if the nation was prepared to exploit it.[3] A large literature about the supposed "revolution in military affairs" quickly developed.

Typical of many intriguing concepts that have enjoyed periods of intense fame, the hullabaloo about the revolution in military affairs largely subsided by the end of the 1990s.[4] However, the idea that information technologies have special implications for warfare remained a subject of serious inquiry that eventually resulted in the recognition of "information operations" and "information warfare" in joint and service doctrines.[5]

Information warfare - as it is defined in joint and service doctrines - is predicated on the belief that the information technologies embedded in new weapons and related sensor and intelligence systems have produced significant military effects at the strategic, operational, and tactical levels of war.[6] These technologies are embedded in a variety of intelligence, surveillance, and reconnaissance (ISR) systems that have already enabled great improvements in detection and precision engagement.[7] Unfortunately, because of the tight linkage of intelligence with surveillance and reconnaissance, information warfare advocates increasingly equate information and intelligence.

The tendency to equate information and intelligence probably stems from the dual nature of the term "intelligence," which is both a process and a range of products. Information and intelligence are epistemologically related concepts, but they differ in terms of their scope, content, and ability to create understanding.[8] As a process, intelligence is a collective description that includes the means to collect data, analyze information, and disseminate products. Reconnaissance and sensor system output is intelligence, but only in a narrow sense. These systems can provide concrete indications of an adversary's presence, capabilities, and dispositions on the ground, on and under the sea, and in the air.[9] No doubt this output, often conveyed in tangible images, has had a major impact on operations. A picture does speak a thousand words. However, sensor output only tells part of the story and the picture can be misleading. Intelligence analysis shows why sensor output and other information collected on the

battlefield is important. Intelligence analysis relates sensor data to the adversary's doctrine, operational history, and probable intentions, in order to help decision makers and commanders understand the strategic, operational, and tactical environments in which they must cope with a dynamic opponent.[10] Intelligence analysis is supposed to provide the understanding that enables information warfare.[11] Joint doctrine for information operations recognizes this relationship.[12] The main issue, however, is whether the intelligence establishment can satisfy the "unique and detailed" demands of information operations and what might happen if it provides inadequate or incorrect intelligence.

The purpose of this study is to examine this complex issue from an organizational standpoint and offer ways to at least mitigate many of the problems inherent in the current relationship between the intelligence and information warfare communities. The organization theory concepts of "bounded rationality" and "complex process coupling" offer ways to identify and analyze some of the inherent limitations of information warfare. The structural constraints that emerged during the post-World War II evolution of the U.S. intelligence community also have implications for the role intelligence can and should play in information warfare. Understanding the logical and structural constraints affecting information warfare and intelligence is the basis for establishing a synergistic harmony between the two disciplines.

CONCEPTS FROM ORGANIZATION THEORY

BOUNDED RATIONALITY

Herbert A. Simon introduced the concept of "bounded rationality," as a qualifier to the "rational actor" model that has been used extensively in political, economic, and organizational analysis.[13] In the rational actor model, a state is assumed to make and execute policies as though it is one entity that knows what it wants and that acts to achieve its objectives at the lowest cost when the opportunity arises. In terms of military affairs, the rational actor perspective assumes that national security decision-makers and military commanders have a clear sense of their priorities, their resources, and opportunities. They have a mission with specific objectives, operational forces with known capabilities, and an adversary with known capabilities and intentions. Friendly and enemy forces meet in an environment that can be observed and measured. As strategic interaction begins or the guns start to fire, the decision makers and commanders issue orders to most efficiently obtain their objectives and complete their missions.

Although Simon recognized the appeal of the rational actor model as a way to simplify complex interactions, he was not satisfied that it reflected the actual behavior of people or organizations. Looking at people, Simon identified three sources of limits which tend to "bound" individual decision makers:

> [He] is limited by his unconscious skills, habits, and reflexes; he is limited by his values and conceptions of purpose, which may diverge from the organization goals; he is limited by the extent of his knowledge and information. The individual can be rational in terms of the organization's goals only to the extent that he is *able* to pursue a particular course of action, he has correct conception of the *goal* of the action, and he is correctly *informed* about the conditions surrounding his actions. Within the boundaries laid down by these factors his choices are rational-goal-oriented.[14]

Simon places particular emphasis on the individual decision-maker's ability to cope with the complexity of the situation, the understanding of the larger goal, and the degree of accurate information received about the situation. People and organizations act with rational intentions to efficiently achieve their personal and organizational objectives, Simon concludes, but physical, psychological, and structural limits make it impossible to attain "perfect information." These individual and organizational constraints have placed bounds on the degree of objective rationality that any decision-maker or organization can hope to achieve.

> In actuality, the human being never has more than a fragmentary knowledge of the conditions surrounding his action, nor more than a slight insight into the regularities and laws that would permit him to induce future consequences from a knowledge of present circumstances.[15]

When decision-makers are faced with this uncertainty and complexity, they often decide to "satisfice" – selecting the first option which nominally meets their criteria, rather than deliberate further to select the best option - assuming that option could ever be fully anticipated in advance.

COMPLEX PROCESS COUPLING

Charles Perrow derived the idea of "coupling" from industrial engineering where it was originally used as a variable to describe chemical plants and oil refineries that made products in elaborate physical plants using complex, closely coordinated, and time dependent processes. Perrow applied the idea of complex process coupling to the study of organizations responsible for complex, technologically intensive, processes.

> Tightly coupled systems have more time-dependent processes: they cannot wait or stand by until attended to. Sometimes this is expressly for efficiency reasons, but generally it is because the production process does not allow for cooling and reheating, for forgetting and then relearning. ...The sequences in tightly coupled systems are more invariant. B must follow A, because that is the only way to make the product. ...In tightly coupled systems, not only are the specific sequences invariant, but the overall design of the process allows only one way to reach the production goal. ...Tightly coupled systems have little slack. Quantities must be precise; resources cannot be substituted for one another; ...failed equipment entails a shutdown because the temporary substitution of other equipment is not possible.[16]

Perrow found that accidents occurred in plants with complex processes even though these plants had been designed with great care and thorough planning. The possible sources of failure had often been correctly anticipated. A valve might stick at one point slowing down the flow of some important component of the process or a display dial might go out of calibration and give a false reading. The system's engineers often correctly identified the potential individual sources of failure in advance; but Perrow discovered that they had not anticipated that combinations of certain failures would have critical interdependencies. Unanticipated combinations produced a special class of "system accidents" that could occur in tightly coupled systems when multiple failures revealed previously unanticipated interdependence between sub-systems or sub-components. The consequences of the subsequent failures were often amplified by the system's human operators who had intervened to correct the initial problem.

The problem became more difficult to solve and potentially more dangerous in proportion to the degree that the system was tightly coupled. Perrow pointed out, "in loosely coupled systems there is a better chance that expedient, spur-of-the-moment buffers and redundancies and substitutions can be found, even though they were not planned ahead of time."[17] A tightly coupled system would provide very limited ability to recover from failure before the process failed completely. Tight coupling put a premium on comprehensive planning and the installation of buffers and automatic recovery systems that could add time for trying different solutions to novel problems.

The amount of difficulty involved in resolving a novel or unanticipated problem varied in terms of the complexity of the process involved and the intricacy of the unanticipated interdependencies that the accident might reveal. Complex interactions involving "unfamiliar sequences, or unplanned and unexpected sequences, ...either not visible or not immediately comprehensible" were particularly difficult problems.[18] Problems of great complexity and intricacy would take much longer to solve and some might never be solved. The situation would become particularly serious if the complex tightly coupled process had a high "catastrophic potential" in that the failure of the system would produce a very destructive outcome. Two examples are the meltdown of a nuclear reactor at Three Mile Island and the leak in the Union Carbide chemical plant in Bophal, India. What is remarkable about system accidents, Perrow concluded, was not their rarity. The conditions that permitted such accidents to occur were so common that they might even be called "normal accidents."[19]

THE NEW ROLE OF INFORMATION IN WARFARE

DOMINANT BATTLESPACE AWARENESS

Impressed with the vivid products of reconnaissance and surveillance capabilities, information warfare advocates argue that information has a new and vastly more significant role in warfare.[20] This belief is based on the expectation that advanced information technologies give strategic decision-makers and commanders the ability to gain a comprehensive view of the overall situation not possible since the days of Napoleon.[21] This comprehensive perspective is called "dominant battlespace awareness" in which the term "battlespace" represents the fusion of the physical and virtual focal points of conflict.

General Gordon Sullivan, a former Chief of Staff of the United States Army, summarized the concept of dominant battlespace awareness as the ability to "locate [the] enemy force quickly and precisely, whether those enemies are agrarian war lords, industrial armies, or an information age peer." At the same time, battlespace awareness also means that armies have the ability to know where their own forces are "much more accurately than before while denying that kind of information to their foes." Lastly, this information is broadly "distributed among all committed forces - land, sea, air, and space - to create a common perception of the battlefield." General Sullivan concludes that this shared "situational awareness, coupled with the ability to conduct continuous operations," has permitted "information age armies to observe, decide, and act faster, more correctly and more precisely than their enemies."[22]

INFORMATION SUPERIORITY

General Sullivan's summation of dominant battlespace awareness consistently points to the ability to see and locate things and to share information about these things with other friendly commanders. The former CSA makes no reference to understanding the implications of the adversary's dispositions, patterns of behavior, or intentions. This is a common attitude among information warfare advocates. In any event, information warfare advocates do not argue that dominant battlespace awareness is sufficient for victory. Instead they note that dominant awareness must be converted into comprehensive "information superiority." Much like air superiority, information superiority must be established within a specific context against a real adversary.

Information superiority is the "capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary's ability to do the same."[23] The concept, however, once again gives little attention to understanding the adversary's intentions. Can information superiority be meaningful if it essentially excludes the adversary's intentions? Michael Herman, a noted intelligence scholar, thinks not. He considers the term "information superiority" quite ambiguous and based entirely on one kind of information: "the observation-measurement of objects." He finds the tendency of information warfare advocates to exclude "the textual or message-like sources that provide access to the enemy's mind" quite remarkable.[24]

Herman also notes that some of the military leaders in the Gulf War found the ability to measure things potentially misleading. General A. C. Horner, for example, the Air Component Commander during Desert Storm, described how the high technology of AWACs radars and moving target indicators provided an opportunity to "inject biases" into judgments about Iraq's intentions and capabilities. Horner observed that "the Gulf War is replete with our failures to understand the enemy, to dissect him with the clarity needed to discover his intentions and capabilities."[25]

Information warfare advocates are not worried about the concerns that General Horner has raised. Instead, they postulate that reconnaissance and surveillance sensors will make centers of gravity self-evident as a result of the identification and location of capabilities.[26]

The lack of attention to the adversary's motivation and intentions also reflects the strong offensive spirit of information warfare. Understanding an adversary's intentions and interests is not particularly important if the capability exists to destroy that adversary at great distance. Similarly, information warfare advocates have apparently suggested that understanding what an adversary wants is irrelevant because the goal of information warfare is the absolute control and domination of that adversary.[27]

CHANGING NATURE OF SPACE AND TIME

At a more subtle level, information warfare advocates also argue that dominant battlespace knowledge and information superiority increase the significance of space and time as variables in warfare. Information technologies have increased space two ways. First, they enable commanders to know the precise location and movements of friendly and adversary forces at a very great range and provide the

ability to strike targets with great precision at these longer ranges. Second, the technologies involved with computer networks also allow operations to take place in the "global information infrastructure." This infrastructure is similar to "cyberspace." Neither is a physical location; but both terms represent the environment in which all sorts of data acquisition and processing capabilities have become interconnected.[28] The ability to conduct "network centric warfare" on an adversary's presence, interests, and resources in the global information infrastructure is one of the more esoteric aspects of information warfare doctrine.[29]

Sensor, strike, and command and control systems also tend to accelerate detection, decision, and action processes, producing a compression of time. Speed becomes a critical variable. Engagements develop faster due to the longer range sensors and terminate quicker due to the increased lethality and range of precision weapons.[30] Similarly, computer network attacks launched into the global information infrastructure possess a time logic all their own.[31]

Changes in the salience of space and time have important implications for command and control. Perceptions of the two variables continuously interact with a commander's awareness of the situation. Space also develops an inverse relationship to time. The logical consequence of this trend is the possibility that physical space and locations become less relevant, while time constraints become ever more dominant.[32]

> [R]apid technological advancement has reduced the span needed to know, decide, and act with the result that time has been shrinking, while space (the extent of the battlefield) has been expanding. This may lead to a state of seamless space, where borders become less relevant in the conduct of war, and time assumes the form of boundaries. This border of time will be the decisive factor of war...[33]

The "front" of classical conception has probably vanished forever, but the zone of conflict - the "battlespace," has expanded tangibly and conceptually. Ironically, given the offensive spirit of information warfare, the density of military forces present on the physical battlefield has also declined significantly. The battlefield has tended to become "empty."[34] Massed armies and fleets will probably never again meet in head-on battle. Extending this trend into the future, battles will increasingly take place across a broadly distributed geographic and virtual reality where smaller and more capable forces engage each other with customized force packages that have become more accurate, longer range, and more deadly.[35]

Highly reliable geographic positioning, reconnaissance, and surveillance systems have allowed friendly forces the ability to rapidly identify, fix, and track adversary movements, dispositions, and preparations in the battlespace. Once located, commanders have the ability to discriminate between the most valuable targets and mass forces on demand in order to attack physical targets with high precision weapons at long range. Some of those weapons may be of the old fashioned variety that destroy through explosive power and shock, but others may be more subtle and achieve destructive effects by corrupting or disabling the adversary's information resources without the use of explosives. Whatever "kill mechanism" a weapon may use, time compression and speed will increasingly characterize engagements

since the objective will be to process all the necessary information required to execute an attack faster than an adversary.

Information warfare advocates claim that the ability to see, think and act more quickly than an adversary has become decisive. A commander's "decision loop" has "tightened" to the point were "an asymmetry created in time proves to be decisive."[36] Time itself has become a factor of vital significance in the information age: "the side that controls time will be in a superior position to conduct war in all dimensions."[37]

IMPLICATIONS OF BOUNDED RATIONALITY AND COMPLEX PROCESS COUPLING

Information warfare advocates posit an idealized rational, value maximizing, decision maker or commander, who exercises information superiority under acute time constraints while dealing with huge volumes of information. This decision maker functions within a technologically rich environment where ISR systems provide fast, accurate, and unambiguous indicators of adversary actions and feedback about the effects of friendly actions. These systems also allow the decision maker to engage and influence the adversary with precision weapons and other information tools at a great distance.

Information warfare advocates admit that things can go wrong in this environment. For example, decision makers and commanders might be swamped by the quantity of information flowing into a command post. However, information warfare advocates do not explicitly acknowledge bounded rationality. Instead they argue that technology-based decision aids can customize the information flow to deliver critical data in a digestible format. They specifically claim that information technology would keep decision makers and commanders informed about the conditions surrounding his actions to an unprecedented level.[38] This seems to respond to two of Simon's qualifications on the attainment of rationality: the ability to understand the goal and the situation.

However, information warfare advocates do not address satisficing. On the contrary, they appear to assume that decision makers and commanders make the best decision and do not select the first alternative which satisfies the minimum conditions. If decision makers and commanders actually satisfice, the anticipated marginal utility of additional investments in esoteric intelligence sensors and command and control systems might be much lower than information warfare advocates assume. Consequently, the additional presumed incremental contribution to "agility" on the battlefield may be much harder to realize than information warfare advocates have considered.

Furthermore, information warfare advocates have not addressed the potential adverse consequences of the tight coupling of ISR systems with precision weapons platforms. Quite the opposite: information warfare advocates emphasize that the speed of this coupling is critical to realize the advantages that come from information superiority. The ability to conduct rapid, precise, and long-range engagement has a strong appeal to commanders who want to reduce "footprints" on the battlefield and increase the mobility and agility of their forces. These commanders, quite rationally, want to achieve the greatest possible impact, at the longest range, in the shortest time with the smallest force. They have

come to believe that ISR systems and information warfare doctrine increase their chances for success and reduce the risk of loss since smaller - but more capable - forces would be exposed to danger for a shorter period of time.

Reality intrudes, unfortunately, because bounded rationality and satisficing establish some very firm limits to the degree of perfectibility of any system which seeks to achieve or apply information superiority. Bounded rationality and satisficing do not suggest that information superiority is a myth; but on a conceptual basis, information superiority may not produce the overwhelming advantage that information warfare advocates expect. Bounded rationality and satisficing behavior make it difficult to ignore the possibility that something may go wrong. If success has become a matter of the ability to "mass on demand" and to execute precision engagements or provide "just in time" resupply, prudent risk management suggests that more redundancy and back up capability should be built into operations than information warfare advocates admit. Likewise, these concepts further suggest that points of diminishing marginal utility exist in the efforts to trade off firepower for precision.

The potential adverse synergy between information warfare, bounded rationality and complex process coupling is evident in a variety of potential "unintended consequences" of information warfare. Some of these consequences have already been identified in information warfare literature.[39] Others consequences derive from studies of the technological acceleration of western society. These consequences can have devastating effects on military operations and strategic interactions.

INFORMATION OVERLOAD

Information warfare advocates recognize the possibility that the amount of information flowing into a headquarters or command post may produce information "overload." In addition to the interaction with bounded rationality, this overload may have a number of procedural consequences. For example, if the volume of information "swamps" the decision making process, the most critical pieces of information may be lost in the volume.[40] This is the same "signal to noise" ratio problem that Roberta Wohlstetter identified in her classic analysis of the intelligence failure that contributed to Pearl Harbor.[41] The introduction of sophisticated presentation technology to tame the data-stream may also disguise missing or incomplete data. In other words, the style of the presentation may obscure its lack of substance or create false confidence.

Rather than reduce bounded rationality, information overload can amplify it. Command centers are already complex technological environments containing numerous communications, intelligence, and administrative systems. Military officers with extensive field experience believe that information overload is already common.[42] Furthermore the addition of new software and hardware to solve information overload problems creates more confusion because it generally increases the information flow.[43] If the flow of information becomes overwhelming, or confidence in the integrity of the data is lost, general uncertainty may lead commanders to ignore information or to be hesitant in using it.[44]

Furthermore, the additional technology that has been introduced to tame the rising datastream has rarely been simple to operate or unambiguous in its output. The amount of additional knowledge that commanders and their staffs must have to properly operate these command and control systems and to understand the feedback that they provide adds to their "knowledge burden." The "knowledge burden" is essentially the price that must be paid in intellectual capital, attention, and manpower, to be sure that the "outcomes of a system are not surprises."[45] Anyone who has attempted to program a video cassette recorder has experienced a knowledge burden. The weight of this burden and where it falls on the staff is directly proportional to the amount of capability that the decision-aid is expected to provide. This, in turn, is usually positively correlated with the complexity of the technology. Some of these decision aids are so complex that they have essentially been accompanied by specialized support personnel from the contractor supplying the system.

Bounded rationality and process coupling are both evident in the consequences of information overload. The new technology introduced into command posts with the intention of making them information warfare capable increases the knowledge burden on the staff which must know how to properly use it. Commanders already work within technically complex command centers. The additional knowledge burden placed on them, or the staff, may incline them to simply turn off the machines, or satisfice, or to make mistakes. In either case, they would demonstrate the restraints of bounded rationality and complex process coupling.

"ROLE OVERLAP" AND MICROMANAGING

The second potential weakness of information warfare in terms of bounded rationality and complex process coupling pertains to the integrity of the command and control hierarchy. Information warfare advocates recognize the requirement for a chain-of-command and a hierarchy of authority. They argue that information technologies will make the chain-of-command more efficient by flattening organizations. However, an organization with a flattened hierarchy may expose subordinates to information that was previously only available to the superior echelon. Access to this information may dispose subordinates to second-guess their superiors and to assume more authority than is appropriate. Alternatively, high resolution details of battlefield activities may be simultaneously broadcast to the highest levels of the hierarchy. This may produce micromanaging in the belief that slight interventions to "fine tune" operations will produce better political outcomes.[46] At the strategic level, such interventions amplify the potential for bounded rationality to manifest itself as "group think." Alternatively, it could produce risk aversion and hesitation in subordinate commanders, who come to expect micromanagement and await what they believe will be inevitable guidance.[47]

The anticipated gains in decentralization and flattened hierarchies that support agility may also be lost because the more likely consequence of enhanced command and control will be centralization. Herbert Simon detected this tendency in most administrative arrangements:

> The difficulties of transmission from sources of information to decision centers tend to draw the latter toward the former, while the difficulties of transmission from decision

> centers to points of action create a pull in the opposite direction. ...The pulls that tend to bring about a centralization of the decision-making functions ...are the need for responsibility, expertise, and coordination. The two principal pulls in the opposite direction - that of decentralization - are, first, the fact that a very large portion of the information that is relevant to decisions originates at the operating level, and second, that the separation of decision from action increases the time and man-power costs of making and transmitting decisions.[48]

Role overlap and micromanaging also reflect complex process coupling. If a subordinate takes an inappropriate initiative, he or she may induce a failure which creates cascading failures at other parts of the operation. By the same token, the tendency of superior echelons to assume greater control through micromanaging can create ambiguity in the subordinate distribution of authority and responsibility for operations. When unanticipated problems arise, this ambiguity may introduce confusion as to which echelon is responsible for problem resolution. Complex and intricate operations are not likely to be successful if there is confusion about the actual distribution of authority and responsibility. Ambiguity in command authority generally does not lead to success.[49]

DECISION PRESSURE AND PROCRASTINATION

The third area of concern pertains to the pressures which information warfare technology places on individual commanders. This consequence speaks directly to bounded rationality. Facing a flood of data, or ambiguous information, commanders may procrastinate and wait for better information to develop. In contrast to satisficing, commanders could develop an "information dependency" that raises the threshold for adequate information prior to making a decision. This dependency could become an information "pathology" if commanders or their staffs reach a point where they are never satisfied that they have enough "actionable information."

The very potential success of information warfare technologies could induce this failure because the expectation of perfection could decrease the effectiveness of commanders in ambiguous or uncertain operational environments.[50] It may be better if commanders do satisfice since the commander who waits for perfect information may be defeated by the one who acts on "good enough" information.[51]

Alternatively, commanders may be overconfident, assuming that a command and control system contains more expertise than it really does. As a result, they may discount expert information that may be available in their staffs or from other organizations supporting their operations. Commanders may also assume that the system has done essential operational coordination for them and that the surveillance and reconnaissance systems have been dedicated to their segment of the mission. This may prove to be untrue at a critical moment.[52]

INAPPROPRIATE LOGIC AND THE PARADOX OF EFFICIENCY

The fourth potential problem of information warfare concerns inappropriate logic and the paradox of efficiency. These are adverse effects of complex process coupling. Information warfare advocates have noted that in order to benefit from acceleration, highly automated systems will be needed to execute a

variety of combat, combat support, and combat service support functions. However, the possibility exists that these systems may make logical, but "inappropriate" decisions that lead to dumb outcomes.[53]

The systems that accelerate the decision making process through automated analysis have great potential to deliver inappropriate logic.[54] For example, surveillance and reconnaissance systems can be programmed to issue an alarm if certain previously defined indicators change. These systems are much more complex than a fire alarm that responds to changes in only two indicators - the presence of heat and smoke. Surveillance and reconnaissance systems are sensitive to numerous inputs distributed over a broad geographic area. Indicators might include increases in the density of moving vehicles, the presence of certain types of radars, or the adversary's sudden use of certain radio frequencies, among many others.

Decision rules are introduced to highlight changes of critical indicators in order to assess what an adversary is about to do. Decision rules are determined in advance based on analysis of the adversary's doctrine, capabilities, presumed intentions, and objectives. The quality of the decision rules built into the system has a direct impact on the ability to overcome the consequences of bounded rationality. The better the decision rules, the faster the system can operate. This is exactly what information warfare advocates want. Ironically, the effort to further perfect decision rules can lead to a "paradox of efficiency" that amplifies the adverse consequences of complex process coupling.

James Gleick introduced the concept of the paradox of efficiency as a way to understand the consequences of efforts made to take slack time out of complex processes in the name of efficiency. Principal examples of such systems are highway and air traffic flow management systems. A paradox of efficiency can produce two outcomes. In the first case, efforts to make the system more efficient are successful. Slack time is removed and the cars, trucks, and planes do move more efficiently, but only for a very short time because the space that is created immediately fills with more cars, trucks, and planes. In other words increasing demand on the system results from every attempt to make it more efficient.

The second version of a paradox of efficiency is the increased potential for a systems accident. In the air traffic industry, for example, spare air crews and aircraft were previously held in reserve to react to a breakdown or weather problems. However, these slack resources were expensive to maintain and were subsequently eliminated to reduce overhead costs. Consistent with the complex process coupling model, a system with no slack has limited flexibility when confronting a novel problem. Today, when weather delays flights or aircraft break down, there are few alternative means to move passengers. With no crews or planes in reserve, airlines have little choice but to cancel flights. Doing so, of course, saves the airline money and passes the cost on to passengers who also have no choice and must pay in time and frustration.[55]

For military operations, the paradox of efficiency suggests that removing reserve capability may be a bad idea because it exacerbates the potential adverse consequences of complex system coupling. It also suggests that the ability to accelerate processes may not always be an intrinsically good idea. The paradox of efficiency and adverse consequences of acceleration were demonstrated in the May 1999 accidental bombing of the Chinese Embassy in Belgrade, Yugoslavia, during the NATO air campaign

against the Milosevic regime. In this case, consistent with information warfare doctrine, air operations were conducted at a very high operational tempo to exert continuous pressure on the Serbian leadership. At the same time, precision weapons focused that pressure on the regime rather than on non-combatants. Consequently, the CIA - in apparently its only attempt to nominate a target - proposed a building in Belgrade believed to contain an important military logistical organization. This target was subsequently approved at the highest level.[56] Unfortunately, the CIA leadership apparently did not know that the logistical unit had moved out of the building and that the Chinese Embassy had moved in. The building was struck with great precision, devastating effect, and catastrophic unintended consequences for international diplomatic relations.[57] Two parts of the system failed simultaneously: an outdated map, and an outdated target database. The possibility was unanticipated. It was a classic example of a systems accident due to the paradox of efficiency and complex process coupling.[58]

Subsequent investigation of the accident revealed the degree to which the acceleration of the target identification and engagement process played a role and the systemic nature of the other causes.[59] It also demonstrated that accuracy thresholds for precision engagements are much harder to achieve and sustain than was previously believed.

ACCURACY THRESHOLDS

The question of information accuracy is particularly serious for ISR systems supporting precision engagements and the global navigation system that supports the precision engagement component of information warfare.[60] Writing four years prior to Chinese Embassy bombing accident, Captain Edward Smith, a career Navy intelligence officer, noted that the accuracy of weapons had already increased much faster than the ability to identify appropriate targets for precision strikes. He concluded that the successful use of precision weapons made intelligence and precision deeply interdependent. Smith noted that: "we must know *which* window/building/time must be targeted - that is, we must know *why* that room in that building at that time is so important to the enemy and how that specific air defense system will attempt to thwart our missile attack."[61]

In contrast to information warfare advocates, Smith doubts that information with this level of accuracy exists within the intelligence system. He further doubts that satellites can rapidly collect and forward this type of information in cases where data bases are incomplete. Lastly he doubts that the amount of information necessary to support precision strike capabilities can be "reduced to neat sets of data that can be handled almost entirely by computer."[62]

Smith's objections directly concern the adverse consequences of complex process coupling. If the ability to increase precision exceeds the ability to understand what is occurring at distant areas of interest, then bounded rationality and complex process coupling will get worse. Unfortunately, as Captain Smith notes, information warfare advocates assert the ability to produce the required information, but they have not proven their case. The Chinese Embassy accident suggests that it may not be possible to prove it.

SYSTEM VULNERABILITY

Misleading lessons drawn from Desert Storm have also created false confidence about the resilience of the surveillance, reconnaissance, and command and control systems supporting information warfare. During Desert Storm, the allies enjoyed "an uncharacteristic free-signaling environment where the major impediments were self-induced."[63] The fact that Iraq let the allies arrange their forces virtually unmolested created a false confidence that the systems are not vulnerable. Quite the reverse is true.

The effort to gain information superiority will be technologically intensive to an unprecedented degree. Dependency on information flows "inevitably creates vulnerabilities an intelligent enemy will not hesitate to exploit."[64] In keeping with Perrow's observations about the linkage of increasingly complex processes, the potential adverse consequences of system vulnerability grows with the level of dependence on the system. Furthermore, opportunities for exploitation increase rather than diminish in relation to the complexity of the technology in use.

Adversaries are likely to appreciate that these systems will become an American operational center of gravity. Consequently, they will focus their destructive attention on exploiting any potential vulnerabilities that they find. Since they are unlikely to seek to match the capability, "asymmetrical responses" will likely be chosen.[65]

"INSTANTANEITY"

Instantaneity is a term used to describe the perceived positive value of acceleration in western society.[66] Instantaneity is evident in the emphasis that information warfare proponents place on the ability to exploit time as represented in the adversary's "decision cycle." The duration of this cycle is an unspecified amount of time between the points when an adversary perceives a problem, makes a decision about that problem, and the adversary's organization implements that decision. Information warfare proponents argue that getting "inside" the opponent's decision cycle is the main objective because it secures the initiative, increases the adversary's uncertainty, and makes him susceptible to control.

Information warfare advocates seem to forget that both the friendly and adversary sides have decision cycles and that both sides are equally prone to bounded rationality. Efforts to get into the adversary's decision cycle are difficult and may also increase the consequences of complex process coupling. Basically each side has two problems in regard to getting "inside" the other's decision cycle.

First, the precise time involved in the decision cycle is unknown and dynamic. Some efforts have been made to measure decision cycles in American command and control systems and the processing efficiency of some adversary command and control systems.[67] However, so many variables may affect the decision process that it is impossible to sort them out in sufficient detail to establish any valid and durable time estimations. Furthermore, decision cycles are likely to be different under emergency circumstances when a higher level of vigilance is achieved.

Second, time itself may not have the same salience for each side. This is particularly true for a less industrialized adversary. Making a virtue of "instantaneity" is very much a western social phenomena.

Western society has developed an obsession for accelerating activities as an end in itself. This acceleration may have little bearing on the intrinsic social value or meaning of the activity itself. From this perspective, Americans tend to rush because it's exciting and it provides an artificial sense of significance and status.[68] Other cultures may operate at a different rhythm that reflects their values and social relationships. Certainly, the Vietnam War demonstrates that a weaker side with a longer time horizon and greater patience can sometimes prevail against a stronger power. In any event, the implication of the instantaneity argument is that the ability to accelerate processes should be applied judiciously. There is no valid reason to rush into a situation simply because it is possible.

Acceleration is expected to be a key advantage of information warfare. However, acceleration also amplifies the adverse synergy of bounded rationality and complex process coupling. This paradox is one of the most serious potential shortcomings of information warfare.

STRUCTURAL CONSTRAINTS AFFECTING INTELLIGENCE SUPPORT FOR INFO WARFARE

The effects of bounded rationality and complex process coupling are present in the criticisms and weaknesses that have been identified in the logic supporting information warfare. Since intelligence is supposed to compensate for some of these weaknesses, the relationship between the intelligence community and the information warfare community becomes that much more significant. The institutional history of the intelligence community since the end of World War II suggests that very powerful structural factors have influenced the way that it has innovated and dealt with uncertainty and complexity.[69]

Many of these factors also have a generally adverse synergy with bounded rationality and complex process coupling because they inhibit the intelligence community's ability to satisfy the demands implicit in the ideal form of information warfare. Overcoming the vested interests and institutional rigidity is a difficult task which will keep intelligence professionals and political leaders occupied for some time to come.

For the sake of this analysis, it is important to understand that intelligence is an "institutionalized" function of government. A number of formally authorized intelligence organizations perform specific tasks according to a mandated division of labor.[70] The collective American intelligence establishment - formally called the "intelligence community" - has been explicitly defined in legislation.[71] The intelligence community has also become an institution in a broader sense. It consists of a professional staff of military and civilian intelligence officers, who share attitudes about proper roles and procedures. The community also has specialized formal organizations. In recent years, a variety of non-government organizations have also begun to perform information gathering and analysis tasks. These organizations have increasingly sought to influence and challenge official policy making.[72]

It is also important to understand that the American intelligence community rose from the ashes of Pearl Harbor at the beginning of World War II and matured during the Cold War.[73] In 1947, when the National Security Act became law, the Cold War was a new and complex problem for the United States.[74] The national political leadership had considerable uncertainty about the Soviet Union's capabilities and intentions. The USSR's secrecy and paranoia amplified this uncertainty. When the Soviet Union

detonated its first atomic bomb in 1949, a general alarm sounded in the west. National Security Council Paper 68 (NSC 68), which was delivered in April 1950, provided a response to the perceived complexity, uncertainty, and danger that the Soviet Union posed. NSC 68 was a catalyst that provided the rationale for the subsequent vast expansion of American political, diplomatic, military, and intelligence capabilities in order to contain the expansionist Soviet Union.[75] NSC 68 was the equivalent of the "big bang" for the intelligence community's universe.

Looking back over the evolution and expansion of the intelligence community during the Cold War, it is apparent that at least four structural factors influenced how the intelligence community defined its mission and priorities, how it organized and specialized, and how it interacted with the political system and economy. These factors are: the need to avoid surprise, confidence in technology, and the establishment of formal specialized organizations.

AVOIDING SURPRISE

In 1947, the Japanese "sneak attack" on Pearl Harbor was a very fresh and vivid memory. By that time, however, atomic bombs were considered the "winning weapon."[76] By extension, a surprise attack with atomic bombs became the ultimate threat and the need to avoid an atomic Pearl Harbor became a compelling objective. In retrospect, it is now known that the Soviet Union did not have the capability to launch a credible short-warning attack against the United States until the 1970s when it developed a sufficient number of reliable and accurate intercontinental ballistic missiles. Nevertheless, fear of the "bolt from the blue" was most acute in the early days of the Cold War. Consequently, the authors of NSC 68 argued that a global intelligence collection campaign was the best way to safeguard against the chance that the Soviet Union might attempt such a surprise attack.

The desire to prevent a Soviet surprise explains many of the subsequent institutional characteristics of the intelligence community because this threat dominated all others. The tremendous expansion of technical collection operations through satellites, aircraft, and ground-based collection systems, were all designed to obtain early-warning information about the Soviet Union's military readiness and intentions. Large bureaucracies were created to manage and perfect these technical sensors.

The intelligence community takes pride in the fact that another Pearl Harbor has not occurred. Unfortunately, the record in avoiding "surprises" of a less devastating nature has not been particularly good and does not provide much reassurance for the future. Alleged intelligence surprises and "failures" have occurred regularly despite the scale of the intelligence effort. The rapid collapse of the Soviet Union was itself apparently an unanticipated surprise. How did the intelligence community fail to sense the internal erosion and fragility within the Soviet regime? How could the most carefully studied and consistently probed adversary in the international system be so weak and unstable without alarms going off all over Washington?

Surprises continue to occur because bounded rationality prevents intelligence organizations and governments from foreseeing all the potential combinations of forces and events that could lead to a unexpected development or surprise. Bounded rationality also suggests that decision makers,

commanders, and intelligence managers are all susceptible to the dominant theories of the day and orthodox thinking.

The one critical advantage that intelligence has to help mitigate the effects of bounded rationality is its analytical function. The degree that intelligence analysis can mitigate bounded rationality depends on the quality of the analysis and the resources dedicated to analysis. The intelligence community originally developed a "redundant" analytical system in which three different organizations: the CIA, the Defense Intelligence Agency, and the Bureau of Intelligence and Research in the State Department, made assessments under a nominal division of labor. This redundancy was tolerated because these agencies had different missions and customers, and because "competitive analysis" was believed to be an antidote for interpretive bias and "group think."[77] Competitive analysis partially compensated for bounded rationality by emphasizing the "all source" nature of the intelligence used in assessments. In other words, contributions from all potential sources of intelligence were evaluated in the course of describing, explaining, and prediction an adversary's behavior.

Unfortunately, the principal intelligence agencies have reduced their analytical resources. This may tend to exacerbate the potential for systems accidents as sources of objectivity are squeezed out of the system.[78] Furthermore, the adverse implications of reduced analysis capability is disguised by the fact that the intelligence community has always favored collection capability over analysis capability. This preference is a consequence of an enduring American faith in technology. [79]

FAITH IN TECHNOLOGY

Colin Gray argues that confidence in a technical "fix" is a traditional article of faith in the American national style of strategy.[80] The authors of NSC 68 shared this confidence and argued for great investments in early warning sensors and surveillance technology as potential "fixes" against a surprise attack. Intelligence collection systems continuously probed and monitored the periphery of the Soviet Union looking for indications of sneak attack preparations and to test the reactions of its intelligence sensors and response capabilities.[81] Technical sensors also evolved into more elaborate and esoteric forms ostensibly to keep pace with advances in military and civilian technologies (e.g. missiles, guidance, telecommunications, nuclear weapons, computers, etc.) that had the potential to change the global balance of power.[82]

The technical "fix" worked very well in the beginning because collection and analysis capabilities were matched. Technical intelligence collection systems obtained information primarily from seeing, counting, and measuring things, like missile silos, ships, airfields, tanks in motorparks, barracks, etc. They also listened to conversations and attempted to intercept "text-based" information that might reveal plans and intentions.[83] Observing and counting things mattered a great deal in assessments of the closed Soviet Union which maintained a level of security vigilance that human espionage agents could penetrate only very occasionally and at very great risk. In the days when the Soviet Union's readiness and capability to launch a decisive surprise or deliberate attack depended on the number of its operational missile silos

and the disposition of its armored forces near the inter-German border, space- based strategic signals and imagery collection capabilities performed admirably.

Nevertheless, problems developed – many of them understandable in terms of complex process coupling and path dependency. Technology became a two edge sword. As technology advanced, the development of greater collection capabilities became and end in itself. Eventually collection capability outpaced the ability to analyze the "take." Simultaneously, technical developments allowed adversaries to shield their communications and conceal their capabilities and intentions.[84] Changes in the global information infrastructure also made it much more difficult for traditional signals intelligence activities to produce the level of detailed information that policy makers came to expect.[85] It is no longer so easy to see the things that need to be counted (e.g. terrorist bases and infrastructure) or to hear the conversations that must be monitored, since they have been encrypted or run through fiber optic systems that do not radiate signals into free space.[86]

Many technical collection capabilities have also proven to be more fragile than anticipated. Other sensors became obsolete more quickly than anticipated. Thomas Behling, the Deputy Director of the National Reconnaissance Office responsible for designing new systems, has already issued an alert concerning major satellite systems.

> Our current generation of satellites is reaching obsolescence and will have to be replaced in the next 5 to 10 years. Given design and development lead-times, decisions about the next generation of reconnaissance satellites are being made now. As a result, by the time the military determines intelligence requirements to supports its new doctrine, it may be too late to influence decisions about the very intelligence support systems upon which the doctrine depends.[87]

In Behling's estimation, the window for the design of new systems is rapidly closing. If new systems are to be customized for information warfare purposes, that work must be done now. However, he is not confident that a coherent plan exists to do this because there is little consensus about what types of new systems are required.[88]

Given the otherwise extensive attention directed to information warfare, Behling's assertion that little attention has been given to synchronizing the design of the next generation of satellites with information warfare requirements is remarkable. Where are the information warfare planners? A tremendous coordination and planning effort must be completed in order to design and develop new satellite systems. The unique nature of these systems and small number that are built also tends to drive up cost. Cost growth might result in further cuts in the number procured. The possibility that an expensive one of a kind satellite might be destroyed in a launch accident is a very considerable additional risk. Even if the system is successfully put into orbit, and works once it gets there, the lower density of systems may reduce the availability of intelligence if crises develop at the same time in widely separated parts of the globe. This is complex process coupling in its pure form.

Obsolescence is also not a unique problem, but it has become more difficult to solve. Dealing with obsolescence in the intelligence community was not a great problem during the Cold War because the

financial backing for strategic reconnaissance systems was almost limitless. New systems were deployed continuously. Spare satellites were often built and launched or kept in reserve for emergency surges. After the Cold War, the situation changed very dramatically. Budgets are still quite large, but losing ground relative to costs and collection continues to be favored over analysis. The picture has changed from a period of redundant and flexible coverage that could compensate for surprises and complex process coupling to a period of relative scarcity.

Information warfare advocates within the military services have noted the declining capability of national intelligence collection systems with concern, but other advocates have dismissed the problem. Since it is now possible to buy satellite pictures with one meter resolution on the ground, they argue that the national imagery system may not be as relevant as it was before.[89] For that matter, intelligence organizations have also started to buy imagery from commercial vendors since it is sometimes easier to buy this imagery than to retarget the declining number of intelligence satellites that are already committed to other missions.[90]

The relative decline of the ability of the national technical collections system to keep up with changes in technology and the growing complexity of the bureaucratic politics and processes involved with replacing and upgrading these systems offers some important lessons for information warfare. First, emphasis on collection must be balanced with equivalent emphasis on the ability to analyze the take. The current imbalance in favor of collection tends to perpetuate the chances for surprises despite the scale of the collection campaign. Second, the fact that new systems are apparently not being designed to maximize their relevance to information warfare fundamentally undermines any claim that information warfare is being pursued as a coherent strategic capability. Third, the availability of imagery from a commercial source in peacetime does not guarantee that the imagery will be available during a crisis. Commercial vendors are also not under the same obligation to insure the accuracy of the information they provide. Finally, technology choices and commitments are often very closely integrated with organizational preferences. When technology choices and organizational preferences become rigidly locked together, the ability to adapt new approaches is stifled.

THE RISE OF SPECIALIZED COLLECTION ORGANIZATIONS

During the Cold War, the investments in technology and fielding of systems simultaneously produced the third structural factor - the establishment of specialized collection organizations. The National Security Agency was established in 1952 to continue signals intelligence activities that the military services conducted in World War II.[91] The CIA had initial responsibility, which it shared with the Air Force, for the development of air and space borne sensors. Ultimately in 1960, the National Reconnaissance Office was established under the Air Force to conduct the air and space imagery collection mission.[92] CIA retained responsibility for control of covert action and clandestine agent espionage operations; but the military services also conducted agent based collection and counterintelligence operations, subject to CIA approval.[93]

The concentration of collection capabilities in specialized organizations tended to "stove pipe" the collection and analysis of information. Each organization was vertically integrated. They controlling the design and operation of its systems, as well as the distribution of its products. While the "competitive analysis" approach compensated somewhat for the "stove pipe" phenomena, the expansion of bureaucratic domains introduced considerable intellectual and organizational rigidity that, in turn, amplified bounded rationality and complex process coupling.

The development of specialized collection agencies has now become a liability because the agencies have become "locked" into their narrowly specialized collection technologies that are too narrowly focused. Furthermore, the agencies cut back analytical resources which reduced their ability to recognize the implications of changes in the strategic environment. They also became encumbered by their own "dogma" and organizational orthodoxy.[94] They have been slow to adopt non-traditional applications of their sensors and to repackage their products to make them quickly available and relevant to the new forms of warfare.[95]

This traditionalism does not bode well for the information warfare advocates who anticipate synergy from non-linear associations and agile multi-tasking. Fortunately, there is some hope that an effective harmony can be established between the current and anticipated capabilities of the intelligence community and the intelligence support requirements of information warfare. This hope is based on the reassertion of the proper role of analysis in command and control and a fundamental reevaluation of the division of labor and responsibility for battlefield information.

ESTABLISHING A HARMONY BETWEEN INTELLIGENCE AND INFORMATION WARFARE

COPING WITH BOUNDED RATIONALITY

There is no escape from bounded rationality, but some conceptual, organizational, doctrinal, and technological changes can be made to help cope with its consequences. For information warfare advocates, the first task is to understand that not all information is created equal. Different types of information have different strengths, weaknesses, and meaning. Surveillance and reconnaissance sensors, for example, may provide moving target indicators of an enemy advance. This is vital warning information that reveals movement, direction, and possibly strength. Imagery from satellites can reveal the types of equipment that the adversary is using which suggests the capabilities that can be brought to bear. Neither source reveal intentions. The intentions of the adversary may be revealed in an intercepted communication or through a clandestine agent. For that matter, the adversary may publicly declare his intentions. At other times, the adversary's intentions may remain a mystery and the subject of hopefully well-informed speculation.

In light of the different types and values of information, advocates must take a hard look at the anticipated benefits of information superiority. They must come to understand that information superiority will not provide automatic understanding of the adversary's intentions. Rather, sensor data and other

inputs must be related to the context of the adversary's prior actions, probable or stated intentions, and a variety of other factors.

Intelligence and operations research analysis helps compensate for bounded rationality by widening the number of minds that examine and assess these indicators. Devil's advocate procedures built into analytical routines can further test the plausibility of conclusions drawn from observations. Analysis is no guarantee that the right answer will be found, but it raises the probability that the quality of the decisions will be improved. These types of procedures should be emphasized in information warfare doctrine, which so far has concentrated on establishing information operations staff relationships and organizations.[96]

The second task for proponents of information warfare is to improve their understanding of the effects of the man-machine interfaces in these systems. Decision aids that tame raging information flows may also increase the knowledge burdens associated with using the aid properly. This knowledge burden may be very tolerable if the decision aid is well designed and fits into the organization's rhythm and purpose. On the other hand, complex decision aids have higher probability for unintended consequences, and aids that are not compatible with the organizational context will only add to the confusion.

Information warfare advocates must also understand that autonomous linkages between target detection and fire control have a great potential for unintended consequences and catastrophic outcomes. These systems may be necessary, but in no case can the speed of any machine be interpreted as a certification of the quality of the data or the validity of the conclusion it reports. As imperfect as human decision making can be, in warfare it is vital to keep a human hand and mind in the loop.

The intelligence community must also take a number of steps to compensate for bounded rationality. First, it must remember that analysis is an intellectual process that takes place in the analyst's mind and in the conversations and coordination that occurs between groups of analysts studying the same problem. It is not a process that can be easily transferred to or replicated in a machine.

Man-machine interfaces are necessary to properly use reconnaissance and sensor systems, but systems must be designed in a manner that permits the analyst to understand the machine's status and the meaning of its output. When intelligence analysis tools become so complex that the analyst "user" becomes the "system operator," a fundamental goal displacement occurs and the machine becomes the analyst.[97] Bounded rationality is bad enough in people, but the catastrophic potential of inappropriate logic in automated intelligence analysis systems is as great as it would be in automatic target engagement systems.

The best way to deal with bounded rationality is to use intelligence analysis as a function and intelligence analysts as individuals in a manner that increases the ability of both to add understanding to military operations and to serve as buffers to maintain positive control. The analysis process and the individual analysts must pay particular attention to the adversary's intentions and the operational environment, and provide critical feedback about the consequences of operations. This includes battle damage assessment.[98]

These are not new roles for intelligence analysis. New roles are not required; the argument here is that the military intelligence leadership must reverse the trend toward the marginalization of analysis that has been induced by the vivid nature of surveillance and reconnaissance technologies. The output of these systems has led some warfighters to conclude that they can be their own intelligence analyst. Military intelligence leaders must convince those who hold this view that it is as dangerous as the one that inspires a doctor to treat himself. The consequences of bounded rationality demand that an effective relationship be established between the sources of understanding and the forces of action. Unfortunately, intelligence leaders have a difficult task because the core argument of information warfare is precisely that information superiority reduces understanding to a product that comes out of a convenient and reliable black box.

The second major step for the national intelligence leadership in terms of compensating for bounded rationality is the restoration of the balance between collection and analysis capabilities. Collection capabilities have been vastly overbuilt and analysis capability has declined dangerously. If budgets and manpower are to be held constant, the only plausible option is to move resources from collection capabilities to increase the analysis base. This is plausible and practicable because the information age does provide many more sources of information that are easier to acquire and use. Current signals intelligence collection must also be more discriminating. The signals intelligence vacuum cleaners have become less effective as a result of the global proliferation of cryptography. Some effort should be maintained at code breaking, but it must be more precisely focused. Sustaining imagery capabilities is required, but some reductions are possible because commercial satellites provide alternative sources. Expansion of human based intelligence should also be considered, but not only in terms of developing clandestine agent networks. The deployment of intelligence officers and military attaches provides overt liaison and coordination capabilities that work with foreign nations. This is less risky in terms of potential political embarrassment, and also recognizes the fact that most human intelligence reporting comes from these types of relationships.

Transferring investments from collection to analysis offers the intelligence community the best hope for separating what is important from background noise. Shifting emphasis from collection to analysis will also be difficult, because big systems develop organizational and technological constituencies that are interested in their perpetuation.[99] Analysis is a function that does not have a natural constituency. The community leadership that the Director of Central Intelligence is expected to provide is the only answer to this structural condition. It is a difficult but critical task.

COPING WITH COUPLING

Information warfare advocates must also realize that complexity and acceleration lead to complex process coupling and - potentially - to systems accidents. The campaign in Kosovo provides excellent reasons to reexamine the information warfare premise that acceleration is good. Operations against the Milosevic regime demonstrate that an adversary can accelerate or decelerate strategic interactions in

ways that can be made immune from friendly influence.[100] Acting faster than the opponent is not always the better course of action.

Time "obsession" is a western social construct. Time is important in warfare, but it only has the salience that information warfare advocates claim when the adversary is a mirror image of the U.S. Only an adversary with the same technologies and the same cultural and social expectations about the value of "instantaneity" will be equally vulnerable to its effects. As the Chinese Embassy bombing example demonstrates, the pressure to act fast and to sustain complex systems, like air tasking order cycles, is replete with the danger of systems accidents.

For information warfare, the best way to mitigate the consequence of complex process coupling is to synchronize operational tempos with the natural rhythm of the strategic interaction that is occurring with the adversary. Information warfare advocates must understand that it is more appropriate to act only as fast or slow as the situation demands. The information warfare "system of systems" must be able to surge and rest as appropriate. If the entire system of systems is sustained at the highest possible speed, it will quickly go into a state of alert fatigue or will need infusions of extraordinary additional resources to maintain hyper vigilance. In any event, hyper vigilance is no panacea, since it can also produce a systems accident.

Contrary to the fundamental tenets of information warfare, the task of creating understanding may mean that the system's tempo must be slowed down in order to increase the amount of time available to make higher quality decisions. It also means moving from a system that is based primarily on brute force information processing power, to a system that balances processing power with conceptual finesse and subtlety. Stepping back from the brink of "instantaneity" may also improve the appreciation for the technological hubris that lies at the heart of information warfare and for the fact that the human capital of decision making systems, as imperfect as it may be, is the component that gives actions meaning and sustains restraint and conscience behind these actions.

The reassertion of intelligence analysis as a vital compliment to operations will also address some of the consequences of complex process coupling.[101] As long as they are not subverted by the pressure and demands from the battlefield operators, analysts in key locations in the command and control system may provide warning when systems errors are developing. For analysts to do this, a new partnership must be established with warfighters for more effective use and placement of analysts.

To establish this partnership, the military intelligence leadership must reevaluate its roles and responsibilities for using information and developing understanding. This reevaluation should result in a more effective division of labor and responsibilities with the proponents of communications, command and control, and fire support functions. Establishing a better division of labor requires the military intelligence leadership to demonstrate vision and discipline because information technology and information warfare doctrine potentially marginalize the value of intelligence analysis.

First, the emphasis on sensor output draws intelligence into a direct support role for fire control. Tension between the intelligence and fire support functions has existed since the first battlefield radars

were deployed. A battlefield radar, which enabled intelligence to see and count approaching forces, also permitted the field artillery to engage distant targets. Bureaucratic fights developed over proponency for these sensors.[102] Intelligence leaders believed radar contributed to understanding the enemy. Weapons proponents believed radar improved the ability to destroy the enemy. The offensive spirit of Army doctrine resolved the argument in favor of the field artillery. For that matter, it would be pointless for a military intelligence leader to argue that intelligence should not support fire control.

The situation with information warfare technologies provides a similar controversy. Are the information technologies servants or masters? The argument presented here is that they must be servants who support a household that is united in its perception of their advantages, liabilities, and proper roles.

Second, escalating specialized communication requirements to move vast loads of information put military intelligence into functional competition with the signal corps. Intelligence leaders, who were frustrated with the inability of the signal community to meet intelligence transmission bandwidth requirements, argued for the development of dedicated signal capabilities. Some impressive systems were acquired. Given the inclination of information warfare advocates to equate information and intelligence, the distinction between intelligence communications and general command and control communications has been blurred. If intelligence analysis has little real or perceived value, than it is logical to see intelligence as redundant and argue for the consolidation of intelligence and signal functions as "information specialists." Unfortunately, this unification would make little contribution to dealing with bounded rationality and would also eliminate a buffer which helps mitigate the chances for systems accidents.

The intelligence community and military intelligence leadership must sharpen the distinction between intelligence analysis, sensor output, and communications services. The military intelligence leadership should engage its operations and communications counterparts in a review of the division of labor and authority for information flows supporting military operations. These functions are obviously interdependent to some degree. The issue is whether the interdependence in these functions is appropriately balanced and integrated. If increasingly dense application of information technologies on the battlefield amplifies the role ambiguity between intelligence, fire control, and signal functions, then complex process coupling will get worse.

If a new and complimentary division of labor can be designed that accounts for the adverse consequences of complex process coupling, then dataflows may be rationalized and practical command and control relationships can be established. Achieving this new balance will probably require very significant reorganization and integration of battlefield intelligence, command and control, and signal capabilities. It will challenge old assumptions about the organization of staffs and the role of combat support organizations. The old "G-staff" structure may no longer be relevant for coordinating these more integrated staff structures. Similarly, hybrid organizations may be needed that more closely integrate the combat support units that provide intelligence and signals services. Reorganization across disciplines is

one of the most difficult tasks that face any military establishment. Even information warfare advocates have shied away from predicting what kind of organizational changes are needed to best utilize these new technologies.

The intelligence community cannot wait to allow the information process to limit the role of intelligence to surveillance and reconnaissance system management, or to marginalize the value of intelligence analysis. The intelligence community must take the lead in helping information users and proponents define the division of labor and authority that must be created to reap the benefits of information warfare while mitigating the consequences of bounded rationality and complex process coupling.

CONCLUSION

Herbert Simon captured the essence of the problem that the intelligence community leadership must help resolve. The intelligence community must challenge the theoretical musings about information warfare that discount the characteristics and capabilities of the human members of the system. Intelligence leaders should remind themselves and information warfare advocates that equal consideration must be given to the human dimension of information warfare and the organizations that have been created to conduct it. The promise of technology that fascinates information warfare advocates, should not cloud an appreciation for the capabilities of human decision-makers:

> For generations to come, although the systems we call organizations will have some mechanized components, their most numerous and most crucial elements will continue to be men. The effectiveness of these systems in handling problems will depend more heavily on the effectiveness of the thinking, problem-solving, and decision-making that men do than upon the operation of the computers and their programs.[103]

As Simon has noted, each human decision-maker is provided with a sizable memory that is stocked cumulatively over a long period of years with various kinds of relevant and irrelevant information, skills, and emotions. Each is able to communicate in natural language with his fellows. Each has the capacity to understand the meaning of their role and their circumstances. Each has courage and - hopefully - the desire to be "good."

Word count: 11,748

ENDNOTES

[1] See: Bernard Brodie, "Technological Change, Strategic Doctrine, and Political Outcomes," in Historical Dimensions of National Security Problems, ed. Klaus Knorr (Lawrence, KS: University Press of Kansas, 1976), 263-306. See also: James Kurth, "A Widening Gyre: The Logic of American Weapons Procurement," Public Policy 19 (Summer 1971): 373-404; Mary Kaldor, "The Weapons Succession Process," World Politics 38 (July 1987): 577-595, and Harvey M. Sapolsky, "Science, Technology and Military Policy," in Science Technology and Society: A Cross Disciplinary Perspective, ed. Ina Spiegel-Rosing and Derek de Solla Price (London: Sage Publications, 1977), 443-471. Also: Alex Roland, "Science and War," Osiris (2d series, 1982): 247-272. Also: Michael Howard, "How Much Can Technology Change Warfare?" in Two Historians in Technology and War, ed. Michael Howard and John F. Guilmartin, Jr. (Carlisle Barracks: U.S. Army War College, Strategic Studies Institute, 20 July 1994): 1-10. At the deepest level there was also speculation that the rise of increasingly robotic and "artificially intelligent" machines had fundamentally altered the relationship between the human race and war. See: Manuel DeLanda, War in the Age of Intelligent Machines (New York: Zone Books, 1991).

[2] David S. Alberts, John J. Garstka and Frederick P. Stein, Network Centric Warfare: Developing and Leveraging Information Superiority (Washington, DC: Department of Defense, C4ISR Cooperative Research Program, 1999), 15. See also: Peter Grier, "Information Warfare: Information May Be the Most Fearsome Weapon on the Emerging Techno-Battlefield," Air Force Magazine 78 (March 1995): 34-37. Also: Eliot Cohen, "A Revolution in Warfare," Foreign Affairs 75 (March/April 1996): 37-54. Martin C. Libicki, What is Information Warfare? (Washington DC: National Defense University, 1995). Also: Michael J. Mazarr, Jeffrey Shaffer, and Benjamin Ederington, The Military Technical Revolution: A Structural Framework: Final Report of the CSIS Study Group on the MTR (Washington: Center for Strategic and International Studies, 1993). Also: Bruce D. Berkowitz, "War in the Information Age," in Information Age Anthology, ed. David S. Alberts and Daniel S. Papp (Washington, DC: National Defense University, 1997): 519-544. Also: James R. FitzSimonds, "Intelligence and the Revolution in Military Affairs," in U.S. Intelligence at the Crossroads, ed. Roy Godson, Ernest R. May, and Gary Schmitt (Washington, DC: Brassey's, 1995): 265-287.

[3] Joseph S. Nye and William A. Owens, "America's Information Edge," Foreign Affairs no. 75 (March/April 1996): 20-26. Admiral William Owens argues that information warfare: "rests on sensing and reporting technologies and includes both the platform and sensors we associate with intelligence gathering, surveillance and reconnaissance - and reporting systems that provide better awareness of our own forces, from in-transit visibility of logistics flows to the location, activity and status of our units, allied units, and noncombatants. Included are an awareness of the weather, terrain and electromagnetic characteristics of any area in which we may use forces." Admiral William A. Owens, "The Emerging System of Systems," US Naval Institute Proceedings (May 1995): 37.

[4] Some skeptics would have predicted this. See: Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions," National Interest 37 (Fall 1994): 30-42. See also: A. J. Bacevich, "Preserving the Well-Bred Horse," National Interest 37 (Fall 1994): 43-49. Also: Gary Stix, "Fighting Future Wars," Scientific American 273 (December 1995): 92-98.

[5] U.S. Joint Chiefs of Staff, Joint Pub 3-13, Joint Doctrine for Information Operations (Washington, DC: Joint Chiefs of Staff, 9 October 1998).

[6] For a summary of these arguments see: Brian Nichiprouk and Carl H. Builder, Information Technologies and the Future of Land Warfare (Santa Monica: Rand Corporation, Arroyo Center, 1995).

[7] Admiral William Owens identified forty five different weapons and related systems which contain these technologies. These systems perform one of three types of function: intelligence, surveillance and reconnaissance (ISR); command control communications computers and intelligence (C4I), or precision force. Detailed assessment of each of these systems is not possible in the scope of this paper. What is

important is the idea that the four principal technologies are expected to have the effect which information warfare advocates postulate. See: Admiral William A. Owens, "Introduction," in Dominant Battlespace Knowledge, ed. Stuart E. Johnson and Martin C. Libicki (Washington, DC: National Defense University, 1995), 5.

[8] For a detailed theoretical appreciation of the role of intelligence in government decision making see: Michael Herman, Intelligence Power in Peace and War (Cambridge: Cambridge University Press, 1996).

[9] Captain Edward A. Smith, a US Navy intelligence officer, notes that the term "intelligence" has also been confused with "surveillance" and "reconnaissance." The acronym "C4ISR" in defense jargon lumps together various systems which provide Command Control Computers Communications [and] Intelligence Surveillance and Reconnaissance. The term suggests that the output of the C4ISR system is a fungible, tightly integrated, and mutually complementary body of knowledge. Smith feels that the presumed unitary nature of the data implied by the acronym C4ISR is actually much more lumpy. C4ISR system output also does not have the analytical value added quality of intelligence. Smith further notes that: "Part of the problem stems from the confusion of the terms 'data,' 'information,' and 'surveillance' with the older term 'intelligence.' The newer terms suggest a degree of precision or black-and-white definition that is seldom the case. By contrast, 'intelligence' defines a process in which raw data is first collated into information and then analyzed to create intelligence. That intelligence product is recognizably and inherently gray - subject to doubt and interpretation and never entirely certain." Edward A. Smith, Jr., "Putting it Through the Right Window," US Naval Institute Proceedings (June 1995): 39.

[10] Robert Jervis emphasizes the dynamic nature of exchanges in the current international security environment. See: Robert Jervis, "Complex System: the Role of Interactions," in Complexity, Global Politics, and National Security, ed. David S. Alberts and Thomas J. Czerwinsky (Washington, DC: National Defense University, 1997): 45-65. See also: Robert Jervis, Systems Effects: Complexity in Political and Social Life (Princeton: Princeton University Press, 1997).

[11] "Understanding" is intelligence according to Edward Waltz. Intelligence and understanding are the product of a three part process hierarchy which advances observation through classification to understanding through analysis. Waltz details the process as follows: "The *observation* process acquires data about some physical process (e.g. combatants on the battlefield...) by the measurement and quantification of observed variables. The observations are generally formatted into *reports* that contain items such as time of observation, location, collector (or sensor or source) and measurements, and the statistics describing the level of confidence in those measurements. An *organization* process converts the data to *information* by indexing the data and organizing it in context (e.g. by spatial, temporal, source, content, or other organizing dimensions) in an information base for subsequent retrieval and analysis. The *understanding* process creates *knowledge* by detecting or discovering relationship in the information that allow the data to be explained, modeled, and even used to predict future behavior... At the highest (and uniquely human) level, *wisdom* is the ability to effectively apply knowledge to implement a plan or action to achieve a desired goal or end state." Edward Waltz, Information Warfare Principals and Operations (Boston: Artech House, 1998): 50-51.

[12] JCS Pub 3-13 identifies the relationship: "The conduct of IO **requires unique and detailed** intelligence never before asked of intelligence collection agencies and activities. **Intelligence preparation of the battlespace** (IPB) is vital to successful IO." JCS Pub 3-13, p. I-18. Emphasis in the original.

[13] Herbert A. Simon, Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations (New York: Free Press, 1976). See also: Herbert A. Simon, "Bounded Rationality and Organizational Learning," in Organizational Learning, ed. Michael D. Cohen and Lee S. Sproull (Thousand Oaks, CA: Sage Publications, 1996): 175-194. See also: James G. March, "Bounded

Rationality, Ambiguity, and the Engineering of Choice," in Decisions and Organizations, ed. James G. March (Cambridge, MA: Basil Blackwell, 1988), 266-293.

[14] Ibid., 241. Emphasis in the original. Simon continues that the rational actor model assumes unattainable levels of knowledge and foresight. Specifically, the rational actor model requires a "complete knowledge and anticipation of the consequences that will follow on each choice." In reality, Simon found that knowledge of consequences is "always fragmentary." Furthermore, "since ...consequences lie in the future," imagination must compensate for missing information based on the assignment of values to future alternatives. He noted that since "values can be only imperfectly anticipated," it is impossible to accurately anticipate all possible alternatives. Since "rationality requires a choice among all possible alternative behaviors," ideal rationality cannot be achieved. Ibid., p. 81.

[15] Ibid.

[16] Charles Perrow, Normal Accidents: Living With High-Risk Technologies (New York: Basic Books, 1984), 94.

[17] Ibid., pp. 94-95.

[18] Ibid., p. 78.

[19] Ibid., p. 257.

[20] See: Stuart E. Johnson and Martin C. Libicki, Dominant Battlespace Knowledge (Washington, DC: National Defense University, 1996).

[21] As one intelligence scholar put it: "[The commander can] once again 'see' the battlefield himself, with a modern equivalent of Napoleon's and Wellington's coup d'oeil, or the maritime legend of Drake's Magic Mirror for seeing over the horizon." Michael Herman, "Where Hath Our Intelligence Been? The Revolution in Military Affairs," Royal United Services Institution Journal (December 1998): 64.

[22] Gordon R. Sullivan and James M. Dubik, War in the Information Age (Carlisle Barracks: U.S. Army War College, Strategic Studies Institute, June 1994), 14.

[23] Waltz, p. 107. Information superiority has four vital consequences which represent the key advantages of information warfare: [1] *Dominant maneuver* - ...agile organizations with high-mobility weapon systems ...attack rapidly at an aggressor's centers of gravity across the full depth of the battlefield. Synchronized and sustained attacks ...[are] achieved by dispersed forces, integrated by an information grid. [2] *Precision engagement* - Near-real-time information on targets ... permit responsive command and control, and the ability to engage and reengage targets with spatial and temporal precision ("at the right place, just at the right time"). [3] *Focused logistics* - Information superiority [means the] efficient delivery of sustainment packages throughout the battlefield, optimizing the logistic process. [4] *Full-dimension protection* - Protection of forces during deployment, maneuver, and engagement ... provide[s] freedom of offensive actions and can be achieved only if superior information provides continuous threat vigilance." Emphasis in original. Waltz, pp. 108-109.

[24] Herman notes that the "explanation of enhanced collection and processing are all in terms of the identification and location of 'things.'" He believes that the capabilities information warriors seek may make battlefield commanders "incredibly well sighted, but in some degree deaf and illiterate in his choice of evidence to assess the enemy." The case for "situational awareness" only becomes convincing, in Herman's view, if it is limited to near "real -time, all-source displays of the location (and some movement) of enemy military equipment and units" which may provide some "major enhancement of commanders'

ability to see battlefields and run battles." However, he believes that "claims that the 'system of systems' provides the deeper kind of 'dominant battlespace knowledge' are less impressive." Herman, pp. 65-67.

[25] Ibid., p. 67.

[26] John Arquilla, "The Strategic Implications of Information Dominance," Strategic Review 22 (Summer 1994): 27.

[27] Ibid.

[28] JCS Pub 3-13, p. GL-6.

[29] For a summary of "network centric warfare" as a sub-discipline of information warfare, see: Alberts, Garstka, and Stein.

[30] The NATO air campaign against Serbia may raise doubts about the relationship between lethality and rapid termination. Evidently some states are more tolerant of pain than information warfare advocates have expected. See: Timothy L. Thomas, "Kosovo and the Current Myth of Information Superiority," Parameters 30 (Spring 2000): 13-29.

[31] For the implications of "tempo" in network centric warfare see: Alberts, Garstka, and Stein, pp. 170-177.

[32] "Throughout history time and space have been played against each other to gain advantage in battle. With the passing of years, time has gradually been compressed while space has expanded." Ajay Singh, "Time: The New Dimension in War," US Naval Institute Proceedings 121 (June 1995): 56.

[33] Ibid., p 59.

[34] Major General Robert H. Scales Jr., America's Army in Transition: Preparing for War in the Precision Age (Carlisle Barracks, Army Issue Paper No. 3, 1999).

[35] Alvin Toffler and Heidi Toffler, War and Anti-War: Survival at the Dawn of the 21st Century (Boston: Little, Brown, 1993), 77.

[36] Singh, p. 57.

[37] Ibid.,. 61.

[38] See: Martin C. Libicki, "DBK and Its Consequences," in Dominant Battlespace Knowledge, ed. Stuart E. Johnson and Martin C. Libicki (Washington, DC: National Defense University, 1995), 46-49.

[39] For a review of the unanticipated consequences of information warfare that have already been identified, see: David S. Alberts, The Unintended Consequences of Information Age Technologies (Washington, DC: National Defense University, 1996).

[40] Ibid., 31-33

[41] See: Roberta Wohlstetter, Pearl Harbor: Warning and Decision (Stanford, CA: Stanford University Press, 1962).

[42] See: Thomas B. Giboney, "Commander's Control from Information Chaos," Military Review 71 (November 1991): 34-38. See also: Jack Burkett, "Tactical Information What You See Is All You Get," Military Review 71 (November 1991): 39-44.

[43] Burkett, p. 39

[44] Alberts, Unintended Consequences, pp. 36-37.

[45] Chris Demchak defines and applies the concept of "knowledge burden" in her study of the U.S. Army's tank modernization program. See: Chris C. Demchak, Military Organizations, Complex Machines (Ithaca: Cornell University Press, 1991).

[46] Political interventions in military operations during the Vietnam War were considered to demonstrate this type of micromanaging. Whether such strategic micromanagement improves outcomes is beyond the scope of this paper.

[47] Alberts, Unintended Consequences, p. 36.

[48] Simon, p. 159.

[49] James March offers a very interesting analysis of ambiguity in command relationships within military organizations. See James G. March and Roger Weissinger Baylon, Ambiguity and Command: Organizational Perspectives on Military Decision-Making (Marshfield, MA: Pitman Publishing Inc., 1986).

[50] Kenneth F McKenzie Jr., "Beyond Luddites and Magicians: Examining the MTR (Military Technical Revolution)," Parameters 25 (Summer 1995): 19.

[51] Decision pressure on commanders may also come from the media, which will be more present on the information age battlefield. This pressure may cause them to act, posture, or seem decisive despite inadequate information. Alberts, Unintended Consequences, p. 39.

[52] Ibid., p. 38.

[53] Ibid., pp. 22-23.

[54] David Alberts points out that computer are "automatons" that have no inherent ability to recognize their own limitations. When applied in inappropriate circumstances, they will produce answers which may be "logical" but quite incorrect. Ibid., p. 40.

[55] James Gleick, Faster: The Acceleration of Just About Everything (New York: Pantheon Books, 1999), 219.

[56] Eric Schmitt, "CIA Says Chinese Embassy Bombing Resulted from Its Sole Attempt to Pick Targets," New York Times, 23 July 1999, p. 10.

[57] Michael Mandelbaum, "A Perfect Failure," Foreign Affairs (September 1999): 2-8. Also: Robert M. Gates, "In War, Mistakes Happen," New York Times, 12 May 1999, p. 25. Also: Eric Schmitt, "CIA Analyst Questioned Target Before Chinese Embassy Bombing," New York Times, 24 June 1999, p. 1.

[58] Mark Thompson, "The Embassy Bombing: Small Steps to a Big Disaster," Time (24 May 1999): 42-43. Eric Schmitt, "Wrong Address of Embassy in Databases," New York Times, 10 May 1999, p. 1. Eric Schmitt, "Smart Bombs, Dumb Map," New York Times, 16 May 1999, sec. 4, p. 6. See also David A. Fulghum, "Intel Mistakes Trigger Chinese Embassy Bombing," Aviation Week and Space Technology (17 May 1999): 34-35. Chuck McCutcheon, "Bombing Mistake Intensifies Calls for Increased Intelligence Funding," CQ Weekly (15 May 1999): 1161-1162.

[59] Somewhat ironically, the U.S. military leadership believed that the allies "were too slow in choosing targets during the war," which tended to slow the tempo of the campaign. Also, "the United States seriously underestimated how many precision-guided munitions would be needed" to achieve sufficient pressure to force the Serbian leadership to capitulate. Elizabeth Becker, "Military Leaders Tell Congress of NATO Errors in Kosovo," New York Times, 15 October 1999, p. 8.

[60] See: Dr. Stanley B. Alterman, "GPS Dependence: A Fragile Vision for US Battlefield Dominance," Journal of Electronic Defense (September 1995): 52-54.

[61] Smith, P. 39 emphasis in original.

[62] Ibid.

[63] Colonel Alan Campen, for example, questions whether Desert Storm is as good an example of information warfare and precision strike as the advocates have argued. Campen agrees that Desert Storm "whetted appetites, fueled expectations and became a fit model for any military force poised to dominate the information spectrum." However, the example requires significant qualification. Campen agrees that U.S. forces created an "information differential," but only after "most of the Free World's commercial communications resources" had been placed in service of the mission and only after "five months of tinkering with sensing, intelligence and communications systems that were designed neither for joint operations nor the stresses of two-sided electronic combat." The allies ability to apply ingenuity and experiment was not hindered by the opponent. Alan D. Campen, "Information Warfare is Rife with Promise, Peril," Signal 48 (November 1993): 20.

[64] Ibid., p. 19.

[65] Scales, p. 5.

[66] Gleick, p. 13.

[67] For example, during the cold war, the U.S. routinely flew monitoring aircraft around the perimeter of the Soviet air defense sensor grid to test its sensitivity and responsiveness. William E. Burrows, Deep Black: Space Espionage and National Security (New York: Random House, 1986), 58-59.

[68] Gleick, p. 12.

[69] For a general review of the readiness of the intelligence community to deal with the information age and efforts to reform intelligence, see: Allan E. Goodman, "The Future of U.S. Intelligence," Intelligence and National Security (October 1996): 645-656. Also Allan D. Goodman and Bruce D. Berkowitz, "Intelligence Without the Cold War," Intelligence and National Security 9 (April 1994): 301-319.

[70] The concept of institutionalized organization was provided by John W. Meyer and Brian Rowan, "Institutionalized Organizations: Formal Structure as Myth and Ceremony," American Journal of Sociology 83 (Summer 1977): 340-363. Furthermore, March and Olsen suggest that it is "possible to seen an institution as the intermeshing of three systems: the individual, the institution, and the collection of

institutions that can be called the environment." James G. March and Johan P. Olsen, Rediscovering Institutions: The Organizational Basis of Politics (New York: The Free Press, 1989), 57.

[71] Mark M. Lowenthal, Intelligence from Secrets to Policy (Washington: CQ Press, 1999), 205-226.

[72] Non-government market research organizations, for example, have performed intelligence activities since the beginning of the stock market. Within the past decade, the significance of these and other "open source" information brokerages has increased very significantly, particularly as a result of the further spread of the Internet.

[73] Birth during a world crisis and maturation in a forty year period of global competition and tension had a significant effect on the intelligence community's institutional values and outlook. Mark Lowenthal notes that this historical experience and particularly the Cold War: "became the major defining factor in the development of most of the basic forms and practices of the U.S. intelligence community. The cold war was ... the predominant national security issue, taking up to half of the intelligence budget... Moreover, the fact that the Soviet Union and its subject allies were largely closed targets had a major effect on U.S. intelligence, forcing it to resort to a variety of largely remote technical systems to collect the required intelligence." For a summary of the major Cold War related events and their influence on the intelligence community, see: Lowenthal, pp. 17-22.

[74] Ibid., p. 12.

[75] Paul H. Nitze, From Hiroshima to Glasnost (New York: Grove Weidenfeld, 1989), 82-100.

[76] See: Gregg Herken, The Winning Weapon: The Atomic Bomb in the Cold War 1945-1950 (Princeton: Princeton University Press, 1981).

[77] Lowenthal, p. 13.

[78] See: Russ Travers, "The Coming Intelligence Failure," Studies in Intelligence (1997).

[79] According to Wesley Wark, a noted intelligence scholar the previous successes of intelligence may have created an over-reliance on technology which could lead to blindness. "The arrival of new means to collect and process information has helped instill a romantic vision of the perfectibility of intelligence. Sharpen the focus, turn the surveillance dials, and one will have the perfect image, and true intelligence assessment. But no intelligence channel carries all the messages needed by governments, and the result of over-reliance on technological wizardry can be complacency, even blindness to threats." Wesley K. Wark, "The Intelligence Revolution and the Future," Studies in Intelligence (1994): 11.

[80] Colin S. Gray, "National Style in Strategy," International Security 6 (Fall 1981): 21-48.

[81] Jeffrey T. Richelson, A Century of Spies: Intelligence in the Twentieth Century (New York: Oxford University Press, 1995), 260-262. See also: Roger C. Dunham, Spy Sub (Annapolis: Naval Institute Press, 1996).

[82] See: Burrows, pp. 227-251.

[83] See: Herman, p. 65.

[84] See: Richard K. Betts, "Intelligence Warning: Old Problems, New Agendas," Parameters 28 (Spring 1998): 26-35.

[85] See: John Hillen, "Know Nothings," National Review (3 August 1998): 28-30. Bruce D. Berkowitz, "The CIA Needs to Get Smart," Wall Street Journal, 1 March 1999, p. 22.

[86] James Risen, "A Top-Secret Agency Comes Under Scrutiny and May Have to Adjust," New York Times, 5 December 1999, p. 1.

[87] Thomas Behling and Kenneth McGruther, "Planning Satellite Reconnaissance To Support Military Operations," Studies in Intelligence (Winter 1998/99): 113.

[88] Behling and McGruther note in addition that: "By the time the military determines intelligence requirements to support its new doctrine [of information superiority], it may be too late to influence decisions about the very intelligence support systems upon which the doctrine depends." Ibid.

[89] Joseph S. Nye, "Peering into the Future," Foreign Affairs (July/August 1994): 86.

[90] William J. Broad, "We're Ready for Our Close-Ups Now," New York Times, 16 January 2000, p. 4.

[91] Jeffrey T. Richelson, The U.S. Intelligence Community (Cambridge: Ballinger Publishing Company, 1985), 11-12.

[92] Burrows, p. 135.

[93] Richelson, A Century of Spies, pp. 244-245.

[94] Bruce Berkowitz notes that: "organizations responsible for developing and applying technology, such as the National Reconnaissance Office (NRO) and the National Security Agency (NSA), have created organizational dogma, and dogma always resist change." Bruce D. Berkowitz, "Information Age Intelligence," Foreign Policy 103 (Summer 1996): 45. See also: Glenn Hastedt, "CIA's Organizational Culture and The Problem of Reform," International Journal of Intelligence and Counterintelligence 9 (Fall 1996): 249-269.

[95] Berkowitz, "Information Age Intelligence," p. 46. Seymour Hersh also notes that the National Security Agency has become a victim of the same technological developments it had helped to develop. He has laid the responsibility for this failure on the "mismanagement" and "arrogance" of the agency's leadership, who showed a "fear of the unknown." They fundamentally failed to prepare for changes in the global information infrastructure. Seymour Hersh, "The Intelligence Gap: How the Digital Age Left Our Spies Out in the Cold," The New Yorker (6 December 1999): 58.

[96] See: JCS Pub 3-13, Chapter V, "Information Operations Planning,"

[97] It is troubling that the Army's flagship military intelligence All Source Analysis System (ASAS) demonstrates many of these complex characteristics. The knowledge burden involved in mastering ASAS is formidable. Training programs at the Army Intelligence Center and School have been revised to accommodate ASAS. Whether ASAS integrates with human-based analysis or has displaced it is an important question that is beyond the scope of this paper.

[98] The controversy over battle damage assessments (BDA) after Desert Storm also indicates the potential organizational biases that have developed by allowing the intelligence centers supporting the theater CINCs to have the primary call in the effectiveness of BDA. See: Travers, p. 43.

[99] See: Thomas L. McNaugher, New Weapons and Old Politics (Washington, DC: The Brookings Institution, 1989).

[100] See: Thomas, pp. 13-29."

[101] For an overview of the role analysis should play in dealing with intelligence problems of the information age see: Allen E. Goodman, Gregory F. Treverton, and Philip Zelikow, In From the Cold: The report of the Twentieth Century Fund Task Force on the future of U.S. Intelligence (New York: The Twentieth Century Fund Press, 1996). See also: Lock K. Johnson, "Analysis for a New Age," Intelligence and National Security (October 1996): 656-661. See also: Paula L. Scalingi, "U.S. Intelligence in an Age of Uncertainty: Refocusing to Meet the Challenge," The Washington Quarterly (Winter 1992): 147-156.

[102] Similar arguments developed within the Army about proponency for unmanned aerial vehicles (UAV). This argument escalated to an interservice conflict when the Army demonstrated a UAV called "Predator" which was as big as a manned airplane and flew for long distances. The Air Force claimed that this UAV required the control of a pilot and therefore should be operated by that service.

[103] Simon, Administrative Behavior, p. 286.

BIBLIOGRAPHY

Books

Alberts, David S. The Unintended Consequences of Information Age Technologies. Washington, DC: National Defense University, 1996.

Alberts, David S., John J. Garstka, and Frederick P. Stein. Network Centric Warfare: Developing and Leveraging Information Superiority. Washington, DC: U.S. Department of Defense C4ISR Cooperative Research Program, 1999.

Burrows, William E. Deep Black: Space Espionage and National Security. NY: Random House, 1986.

DeLanda, Manuel. War in the Age of Intelligent Machines. New York: Zone Books. 1991.

Demchak, Chris C. Military Organizations, Complex Machines. Ithaca: Cornell University Press, 1991.

Dunham, Roger C. Spy Sub. Annapolis: Naval Institute Press, 1996.

Gleick, James. Faster: The Acceleration of Just About Everything. New York: Pantheon Books, 1999.

Goodman, Allan E., Gregory F. Treverton, and Philip Zelikow. In From the Cold: The Report of the Twentieth Century Fund Task Force on the Future of U.S. Intelligence. New York: The Twentieth Century Fund Press, 1996.

Herken, Gregg. The Winning Weapon: The Atomic Bomb in the Cold War 1945-1950. Princeton: Princeton University Press, 1981.

Herman, Michael. Intelligence Power in Peace and War. Cambridge: Cambridge University Press, 1996.

Jervis, Robert. System Effects: Complexity in Political and Social Life. Princeton: Princeton University Press, 1997.

Johnson, Stuart E. and Martin C. Libicki. Dominant Battlespace Knowledge. Washington, DC: National Defense University, 1995.

Libicki, Martin C. What is Information Warfare? Washington, DC: National Defense University, 1995.

_____. Illuminating Tomorrow's War: McNair Paper 61. Washington, DC: National Defense University, October 1999.

Lowenthal, Mark M. Intelligence From Secrets to Policy. Washington, DC: Congressional Quarterly, 1999.

March, James G., and Johan P. Olsen. Rediscovering Institutions: The Organizational Basis of Politics. New York: Free Press, 1989.

March, James G. and Roger Weissinger Baylon. Ambiguity and Command: Organizational Perspectives on Military Decision-Making. Marshfield, MA: Pitman Publishing Inc., 1986.

Mazarr, Michael J., Jeffrey Shaffer, and Benjamin Ederington. The Military Technical Revolution: A Structural Framework: Final Report of the CSIS Study Group on the MTR. Washington: Center for Strategic and International Studies, 1993.

McNaugher, Thomas L. New Weapons and Old Politics. Washington, DC: The Brookings Institution, 1989.

Nichiprouk, Brian, and Carl H. Builder. Information Technologies and the Future of Land Warfare. Santa Monica: Rand Corporation, Arroyo Center, 1995.

Nitze, Paul H. From Hiroshima to Glasnost. New York: Grove Weidenfeld, 1989.

Perrow, Charles. Normal Accidents: Living With High-Risk Technologies. New York: Basic Books, 1984.

Richelson, Jeffrey T. The U.S. Intelligence Community. Cambridge: Ballinger Publishing Company, 1985.

_____ A Century of Spies: Intelligence in the Twentieth Century. New York: Oxford University Press, 1995.

Scales, Major General Robert H. Jr. America's Army in Transition: Preparing for War in the Precision Age. Army Issue Paper No. 3, Carlisle Barracks: 1999.

Simon, Herbert. A. Administrative Behavior: A Study of Decision-Making Processes in Administrative Organizations. New York: The Free Press: 1976.

Toffler, Alvin, and Heidi Toffler. War and Anti-War: Survival at the Dawn of the 21st Century. Boston: Little, Brown, 1993.

Waltz, Edward. Information Warfare Principals and Operations. Boston: Artech House, 1998.

Wohlstetter, Roberta. Pearl Harbor: Warning and Decision. Stanford, CA: Stanford University Press, 1962.

Articles in Edited Books

Berkowitz, Bruce. "War in the Information Age." In Information Age Anthology, ed. David S. Alberts and Daniel S. Papp, 519-544. Washington, DC: National Defense University, 1997.

Brodie, Bernard. "Technological Change, Strategic Doctrine, and Political Outcomes." In Historical Dimensions of National Security Problems, ed. Klaus Knorr, 263-306. Lawrence, KS: University Press of Kansas, 1976.

FitzSimonds, James R. "Intelligence and the Revolution in Military Affairs." In U.S. Intelligence at the Crossroads, ed. Roy Godson, Ernest R. May, and Gary Schmitt, 265-287. Washington, DC: Brassey's, 1995.

Jervis, Robert. "Complex Systems: the Role of Interactions." In Complexity, Global Politics, and National Security, ed. David S. Alberts and Thomas J. Czerwinski, 45-65. Washington: National Defense University, 1997.

Libicki, Martin C."DBK and Its Consequences." In Dominant Battlespace Knowledge, ed. Stuart E. Johnson and Martin C. Libicki, 23-50. Washington, DC: National Defense University, 1995.

March, James G. "Bounded Rationality, Ambiguity, and the Engineering of Choice." In Decisions and Organizations, ed. James G. March, 266-293. Cambridge, MA: Basil Blackwell, 1988.

Owens, Admiral William A., "Introduction." In Dominant Battlespace Knowledge, ed. Stuart E. Johnson and Martin C. Libicki, 1-14. Washington, DC: National Defense University, 1995.

Sapolsky, Harvey M., "Science, Technology and Military Policy." In Science Technology and Society: A Cross Disciplinary Perspective, ed. Ina Spiegel-Rosing and Derek de Solla Price, 443-471. London: Sage Publications, 1977.

Simon, Herbert. "Bounded Rationality and Organizational Learning." In Organizational Learning, ed. Michael D. Cohen and Lee S. Sproull, 175-194. Thousand Oaks: Sage Publications, 1996.

Journal and Newspaper Articles

Arquilla, John. "The Strategic Implications of Information Dominance." Strategic Review 22 (Summer 1994): 24-30.

Alterman, Stanley B. "GPS (Global Positioning System) Dependence: A Fragile Vision for US Battlefield Dominance." Journal of Electronic Defense 18 (September 1995): 52-54.

Bacevich, A. J. "Preserving the Well-Bred Horse." The National Interest (Fall 1994): 43-49.

Becker, Elizabeth. "Military Leaders Tell Congress of NATO Errors in Kosovo." New York Times, 15 October 1999, p. 8.

Behling, Thomas. And Kenneth McGruther. "Planning Satellite Reconnaissance to Support Military Operations." Studies in Intelligence (Winter 1998): 113-121.

Berkowitz, Bruce D. "Information Age Intelligence." Foreign Policy 103 (Summer 1996): 35-50.

_____. "The CIA Needs to Get Smart." Wall Street Journal,1 March 1999, p. 22.

Betts, Richard K. "Intelligence Warning: Old Problems, New Agendas." Parameters 28 (Spring 1998): 26-35.

Broad, William J. "We're Ready for Our Close-Ups Now." New York Times, 16 January 2000, sec. WK, p. 4.

Burkett, Jack. "Tactical Information What You See Is All You Get." Military Review 71 (November 1991): 39-44.

Campen, Alan D. "Information Warfare is Rife with Promise, Peril." Signal 48 (November 1993): 19-20.

Cohen, Eliot. "A Revolution in Warfare." Foreign Affairs 75 (March/April 1996): 37-54.

Fulghum, David A. "Intel Mistakes Trigger Chinese Embassy Bombing." Aviation Week and Space Technology (17 May 1999): 34-35.

Gates, Robert M. "In War, Mistakes Happen." New York Times, 12 May 1999, p. 25.

Giboney, Thomas B. "Commander's Control from Information Chaos." Military Review 71 (November 1991): 34-38.

Goodman, Allan E. "The Future of US Intelligence." Intelligence and National Security (October 1996): 645-656.

Goodman, Allan E., and Bruce D. Berkowitz. "Intelligence Without the Cold War." Intelligence and National Security 9 (April 1994): 301-319.

Gray, Colin S. "The Changing Nature of Warfare?" Naval War College Review 49 (Spring 1996): 7-22.

Grier, Peter. "Information Warfare: Information May Be the Most Fearsome Weapon on the Emerging Techno-Battlefield." Air Force Magazine 78 (March 1995): 34-37.

Hastedt, Glenn. "CIA's Organizational Culture and The Problem of Reform." International Journal of Intelligence and Counterintelligence 9 (Fall 1996): 249-269.

Herman, Michael. "Where Hath Our Intelligence Been? The Revolution in Military Affairs." Royal United Services Institution Journal (December 1998): 62-68.

Hersh, Seymour M. "The Intelligence Gap." The New Yorker, 6 December 1999, p. 58.

Hillen, John. "Know Nothings." National Review (3 August 1998): 28-30.

Johnson, Loch K. "Analysis for a New Age." Intelligence and National Security (October 1996): 657-671.

Kaldor, Mary. "The Weapons Succession Process." World Politics 38 (July 1987): 577-595.

Krepinevich, Andrew F. "Cavalry to Computer: The Pattern of Military Revolutions." National Interest 37 (Fall 1994): 30-42.

Kurth, James. "A Widening Gyre: The Logic of American Weapons Procurement." Public Policy 19 (Summer 1971): 373-404.

Mandelbaum, Michael. "A Perfect Failure." Foreign Affairs (September 1999): 2-8.

McCutcheon, Chuck. "Bombing mistake intensifies calls for increased intelligence funding," CQ Weekly, (15 May 1999): 1161-1162.

McKenzie, Kenneth F., Jr. "Beyond Luddites and Magicians: Examining the MTR (Military Technical Revolution)." Parameters 25 (Summer 1995): 15-21.

Meyer, John W. and Brian Rowan. "Institutionalized Organizations: Formal Structure as Myth and Ceremony." American Journal of Sociology 83 (Summer 1977): 340-363.

Nye, Joseph S. "Peering into the Future." Foreign Affairs (July/August 1994): 82-93.

Nye, Joseph S. and William A. Owens. "America's Information Edge." Foreign Affairs 75 (March/April 1996): 20-36.

Owens, William A., Admiral. U.S. Navy (Ret.), "The Emerging System of Systems." US Naval Institute Proceedings (May 1995): 1-4.

Risen, James. "A Top-Secret Agency Comes Under Scrutiny And May Have To Adjust." New York Times, 5 December 1999, p. 1.

Roland, Alex. "Science and War." Osiris (2d series, 1982): 247-272.

Scalingi, Paula L. "U.S. Intelligence in an Age of Uncertainty: Refocusing to Meet the Challenge." The Washington Quarterly (Winter 1992): 147-156.

Schmitt, Eric. "Smart Bombs, Dumb Map." New York Times, 16 May 1999, sec. 4, p. 6.

_____ "CIA Says Chinese Embassy Bombing Resulted from Its Sole Attempt to Pick Targets." New York Times, 23 July 1999, p. 10.

_____ "Wrong Address of Embassy in Databases." New York Times, 10 May 1999, p. 1.

_____ "CIA Analyst Questioned Target Before Chinese Embassy Bombing." New York Times, 24 June 1999, p. 1.

Singh, Ajay. "Time: The New Dimension in War." JFQ:" Joint Forces Quarterly 10 (Winter 1995-1996): 56-61.

Smith, Edward A., Jr. "Putting it Through the Right Window." U.S. Naval Institute Proceedings 121 (June 1995): 38-40.

Stix, Gary. "Fighting Future Wars." Scientific American 273 (December 1995): 92-98.

Thomas, Timothy L. "Kosovo and the Current Myth of Information Superiority." Parameters 30 (Spring 2000): 13-29.

Thompson, Mark. "The Embassy Bombing: Small Steps to a Big Disaster." Time (24 May 1999): 42-43.

Travers, Russ. "The Coming Intelligence Failure." Studies in Intelligence (1997): 40-50.

Wark, Wesley K. "The Intelligence Revolution and the Future." Studies in Intelligence (1994): 9-16.

Government Documents

Howard, Michael. "How Much Can Technology Change Warfare?" In Two Historians in Technology and War. ed. Michael Howard and John F. Guilmartin, Jr., 1-10. Carlisle Barracks: U.S. Army War College, Strategic Studies Institute, 20 July 1994.

Sullivan, Gordon R., and James M. Dubik. War in the Information Age. Carlisle Barracks: U.S. Army War College, Strategic Studies Institute, June 1994.

U.S. Joint Chiefs of Staff. Joint Pub 3-13, Joint Doctrine for Information Operations. Washington, DC: U.S. Joint Chiefs of Staff, 9 October 1998.